RHIC Operations Procedures Manual
AGS Operations Procedures Manual

4.91 CONFIGURATION MANAGEMENT PLAN FOR THE PARTICLE ACCELERATOR SAFETY SYSTEM

Text Pages 1 through 9

Hand Processed Changes

HPC No.	Date	Page Nos.	Initials

Revision No. 4 Approved:

Satoshi Ozaki 6/1/99
RHIC Project Director Date

Concurrence: Derek Lowenstein 6/2/99
AGS Department Chair Date

Preparer(s): S. Musolino

Date Issued: June 1, 1999
RHIC-OPM 4.91 - Category A
AGS-OPM 4.91 (Y)

4.91 Configuration Management Plan for the Particle Accelerator Safety System

1.0 Purpose and Scope

This document describes the method by which changes to the Particle Accelerator Safety System (PASS) hardware, software, appropriate documentation and technical baselines are determined, maintained and changes to those baselines are controlled, documented and approved. These requirements are in addition to the RHIC Configuration Management Plan.

Until the RHIC Project and the AGS Department are consolidated, replace the generic term "Department" with either "AGS" or "RHIC," as appropriate.

2.0 Responsibilities

2.1 Prior to implementation of any changes to previously baselined PASS hardware or software system logic, the cognizant Department Engineer-in-Charge of the Safety System (ECSS) is responsible to request they be reviewed and approved.

2.2 The Radiation Safety Committee (RSC) is responsible for the review of PASS in accordance with the Committee charge in AGS OPM 1.10, Attachment 8.1 and additional guidance in a memorandum from Ozaki and Lowenstein to Reece dated June 21, 1996.

2.3 Independent engineering review and implementation of the cognizant Safety Committee recommendations are the responsibility of RHIC Project Management, AGS Department or the successor department, as appropriate.

2.4 The Cryogenic Safety Committee (CSC) is responsible to review any conceptual design changes that affect the Oxygen Deficiency Hazard (ODH) monitoring or emergency ventilation system operation.

2.5 The Accelerator Systems Safety Committee (ASSC) is responsible for reviewing State Tables, software and the engineering of hardware.

2.6 The RSC Chair is responsible for reviewing this procedure in a manner consistent with the review cycle for the RSC procedures.

3.0 Prerequisites

None

4.0 Precautions

None

5.0 Procedure

5.1 Technical Baseline and Change Control Procedure

The Department ECSS shall prepare drawings, specifications, test procedures, and other design documents which present a verifiable engineering description of the Baseline PASS hardware. These drawings, specifications, test procedures, and other design documents shall be prepared in conformance with standard RHIC Project or the successor department formats for such documentation.

5.2 Change Control Process

A. Proposed changes to PASS hardware, software, Baselined specifications, drawings or test procedures with an A1 (Critical) QA Classification Category shall be documented on a Class I Engineering Change Request (ECR) form by the Department ECSS or designee. Processing of the ECR shall be in accordance with the RHIC Project or successor department Configuration Management Plan with the following additions:

Review of Changes

i. The Department ECSS shall review, and submit the proposed change to the ASSC Chair. The change shall be fully described with any necessary supporting documentation. A copy of the proposal shall also be submitted to the RSC Chair.

ii. All proposed modifications, test procedures or changes in technical specifications shall be reviewed by a sub-committee appointed by the ASSC.

iii. Any modification that affects the conceptual design for ODH monitoring or emergency ventilation operation shall be reviewed by the CSC and the CSC Chair or designee shall sign the ECR/ECN.

iv. All temporary hardware changes shall be processed in accordance with RHIC OPM 4.92.

v. The RHIC ASSC shall conduct engineering reviews of changes to software, component substitution and replacement, hardware and State Tables.

vi. The RSC Chair shall make a determination if RSC review of issues in step v. is required.

vii. The review (sub)committee shall determine whether the proposed change(s) suggest retraining of the Main Control Room (MCR) Operations staff and/or other personnel and determine any impacts to operation procedures.

viii. The RHIC ASSC Chair or designee shall assure that ECR/ECN documentation conforms to the RSC sub-committee recommendations. Proposed changes are subject to an appropriate independent engineering review as required by RHIC Project or successor department Management.

ix. If the RHIC ASSC Chair concurs with the proposed change, the ECR shall be signed and forwarded to the department Management for processing. The ECR shall be converted to an Engineering Change Notice (ECN) and shall be sent to the Department ECSS as specified by the department Configuration Management Plan. In addition to the standard distribution, a copy shall be sent to the RSC File.

x. Approved and verified changes of any type shall not be incorporated into the baselined drawings, specifications, test procedures, State Tables or other design documents until the successful completion of Step 5.3.

xi. Requirements for retesting following alterations to baselined PLC programs shall fall into one of the three following categories:

1. Category 1 - This level of code change has altered the basic functionality of a safety related portion of the code. Retesting and recertification of the affected PLC code is required. The extent of retesting necessary to recertify the altered code shall be determined by the RSC Chair or his designee.

2. Category 2 - This level of code change has not changed the functionality of a safety related portion of the code, but has altered an ancillary function. Examples are timer value changes in the portion of the code that report the status of a fan or vent, or code that controls the TV system. The RSC Chair or his designee shall convene a panel of experts to review the ladder logic to determine the extent of the changes necessary and the locations within the code that require change. Oversight of the actual code changing process by the PASS software engineer shall also be provided by the RSC panel. The extent of retesting necessary to recertify the altered code shall be determined by the RSC Chair or his designee.

3. Category 3 - This level of code change has changed the program check sum, but has not altered any safety functionality or any other function within the operational software. Examples of this type of code change are amendments to the software title or access passwords. Retesting following Category 3 code changes is not necessary.

B. A description of the change shall be put into the PASS Engineering Change Logbook.

C. If an approved change affects the current system test procedures, the test procedure shall be revised in accordance with the RHIC OPM 1.4 or successor department procedure. RSC review and concurrence is required on all revised test procedures. The Department ECSS shall determine if the change affects the test procedures. The RSC Chair shall review the determination.

5.3 Functional Test of Changes to the System

5.3.1 Functional tests of hardware and software shall be approved by the RSC or ASSC, as appropriate.

5.3.2 Prior to beam or cryogenic operation, documentation that adequately describes the results from the functional test of any hardware or software modification shall be submitted for review to the RSC or CSC, as appropriate, by the Department ECSS. The Maintenance Panel View Display (PVD) is exempt unless it contains command code.

5.3.3 If during functional testing a mechanical repair, which is a replacement by an identical device/component, must be made that would not require changes to the baselined drawings, specifications, test procedures, or other design documents, the functional testing shall proceed. A record of the repair shall be maintained by the Department ECSS. The RSC and/or ASSC Chair, as appropriate, shall be informed of the repair by the Department ECSS and a determination on whether supplemental testing is necessary shall be made by them.

5.4 Hardware Security and Labeling

A. All PASS enclosures shall be secured with the same lock/key combination. The number of operational keys to be retained shall be determined by the Department ES&H Coordinator. Excess keys shall be destroyed under his supervision, and the remaining copies of the enclosure key shall be sequentially numbered. Accountability of these remaining keys shall be strictly maintained. The Department ES&H Coordinator may issue keys to PASS Group personnel who are authorized to access the PASS enclosures, and a method of maintaining strict control and accountability of issued keys shall be developed by him. One set of numbered maintenance keys shall be kept in the Building 911 QA safe, and another set in the 1005S RHIC ECSS safe. All spare numbered keys shall be kept by the Department ES&H Coordinator in his lockbox.

B. Except for the operational CA, Sweep and S keys in the key tree in the Main Control Room and the maintenance keys kept in the safe, the spare sweep, CA and S keys shall be kept by the department ES&H Coordinator or successor in the lockbox.

CAUTION

Copies of controlled keys cannot be issued without consultation with the RSC Chair and RHIC and/or AGS Management, or successor department, as appropriate. Unauthorized use of a spare key could result in a grave danger to the user and will prompt disciplinary action.

C. The enclosures, wiring, interlocked chipmunks, etc., shall be appropriately labeled with Orange Tags so as to identify them as part of PASS. Critical devices, and any other appropriate device, shall be labeled with numbered Orange Warning Tags per applicable steps in AGS OPM 4.15.

D. Any baselined software or hardware found to deviate from the approved design basis shall be documented on a BNL Inspection/Test Record form and immediately reported to the RSC Chairman, the Department ECSS, the Assistant to the RHIC Project Director for ES&H and AGS Associate Chairman for Safety. The deviation shall be evaluated by the Facility Manager, for DOE reportability, as appropriate.

CAUTION

If a deviation from the approved design is present, then unsafe operation of the system may occur. RS LOTO of the area per AGS OPM 9.1.16 shall be required until a review is conducted by the RSC.

E. During accelerator operations, the Operations Coordinator may give permission for the Department ECSS or designee to unlock equipment racks or the 911B security area containing PLC devices for the limited purpose of inspection. Access shall be limited to only one PLC Division cabinet at a time. During cryogenic only operation, the department ES&H Coordinator, Assistant to the RHIC Project Director for ES&H or designee shall give permission to access the aforementioned enclosures for the purpose of inspection. During times of non-operation, access may be supervised by the Department ECSS. When any key is removed/returned to either safe, it shall be logged in the Safe Logbook. This logbook shall be provided for each safe by the Department ECSS and the Quality Assurance Representative.

F. The safe in the office of the Department ECSS in Building 1005 and the safe in the office of the QA Representative may each contain a set of Sweep and CA keys, whose purpose is to facilitate PASS system test procedure execution. During accelerator shutdown, after confirmation of appropriate RS LOTO, or during maintenance periods, after confirmation by the duty Operations Coordinator of RS LOTO, the Department ECSS may remove these keys for the duration of active testing. During cryogenic only operations when testing is expected to take place within RHIC cryogenic areas, the approval of the department ES&H Coordinator, Assistant to the RHIC Project Director for ES&H or designee is also required. When any key is removed/returned to either safe, it shall be logged in the Safe Logbook. This logbook shall be provided for each safe by the Department ECSS and the quality Assurance Representative.

5.5 Control System of Documentation and Software

A. Upon authorized baselining by the Department ECSS, the PLC source code and relevant documentation shall be maintained per the requirements of this document.

B. The date and revision of the current compiled code shall be documented to the cognizant department Management and the RSC Chairman by the Department ECSS. A Release History Log shall be maintained by the Department ECSS.

C. One master copy and one verified duplicate copied from the master of the PLC source and compiled code, the compiler program on which the operation/compilation of the Safety System depends, and documentation describing the configuration of the programming hardware (e.g., hardware type, operating system, etc.) shall be maintained. The master and the copy disks shall be write protected and conspicuously marked by color coding, date and revision number. When the storage medium is CD ROM, a second CD ROM obtained from the vendor can be used for backup storage. Backup files shall also be stored in the Computing & Communication Division (CCD) Automated Backup and Restore System (ABARS) or backed up on a network server.

D. The location of the two official copies are as follows: the master copy shall be secured in a fire retardant safe in the office of the Department ECSS in Building 1005. Duplicates of the masters shall be secured in a fire retardant safe in the Quality Assurance Office in Building 911. The PLC source code may be removed from either safe by the duty Operations Coordiantor (OC) or the Head of MCR, with permission of the SSSH or QA Representative or Head of Safety Section (HOSS) or RSC Chairman or the Assistant to the RHIC Project Director for ES&H or Department Chair Office. When system software disks are removed/returned to either safe, it shall be logged in the safe logbook. This logbook shall be provided for each safe by the Department ECSS and the Quality Assurance Representative.

E. A printout of the baselined State Tables and Operating Modes of the A and B Division shall be maintained in the office of the Department ECSS. This documentation shall be identified by date and revision level.

NOTE ***It is not a requirement that Ladder Diagrams be generated for all subsequent revisions. An updated copy will be generated upon request.***

F. Current revision hard copies and/or electronic versions of the State Tables and Operating Modes shall be provided to the MCR.

G. Control of baselined drawings and the State Tables shall be maintained by the Collider Ring Design Room, with copies made available in Read-Only format via the Configuration Control Board file system.

5.6 Control of Special PASS Test Equipment

Except for standard tools, voltmeters, etc., any dedicated devices which could degrade functionality that are needed for system testing; i.e., special jumper/clips, mechanical door switch bypasses, etc., shall be:

A. Predefined in the respective test procedure.

B. Kept in the safe in either the office of the Department ECSS in Building 1005, or in the Quality Assurance Office in Building 911.

C. Verified they are back in the safe via a signature on the appropriate test procedure by the Department ECSS or designee.

5.7 A PASS System Trouble Logbook shall be maintained to track problems discovered during the test and operational phases of PASS.

A. Problems found during testing of PASS shall be tracked by entering them in the Logbook. Marginal or compilation notes made in the Test Procedure sheets for problems that require correction shall be transcribed into the Logbook.

B. Problems found during PASS operation shall be immediately reported as required in 5.4.D. Problems shall also be entered in the Logbook.

CAUTION

If a deviation from the approved design is present, unsafe operation of the system may occur. RS LOTO of the area per AGS OPM 9.1.16 may be required until a review is conducted by the RSC.

C. Each entry in the Logbook shall be assigned a unique tracking number.

D. For facilitation of tracking and auditing, the first page(s) of the Logbook shall consist of an index which lists all problems by tracking number and their current dispositions.

E. Only one copy of the Logbook shall exist, and it shall be in the custody of the Department ECSS. It shall be his responsibility to keep the Logbook current and to ensure that all pertinent entries are made, tracked and corrected.

6.0 Documentation

6.1 PASS Engineering Change Logbook
6.2 RSC File
6.3 Baselined Schematics, State Tables and Ladder Diagrams
6.4 System Trouble Logbook
6.5 System Release History Logbook
6.6 System Work in Process Logbook
6.7 Safe Logbook
6.8 PASS System Trouble Logbook

7.0 References

7.1 RHIC Project Configuration Management Plan
7.2 RHIC Design Standard DS-1
7.3 AGS OPM 4.15 AGS Access Control System Modifications and Bypass
7.4 AGS OPM 9.1.16 Lockout/Tagout for Radiation Safety
7.5 ES&H Standard 1.5.3

8.0 Attachments

None

Fill Out Reading Acknowledgment Form